SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

INTERNAL SECURITY INCIDENTS DETECTED IN COMPANIES USING SEARCHINFORM SERVICES

Data for the first half of 2020

SearchInform has analyzed the most frequent types of internal information security incidents. They include attempts of a data breach, corporate fraud, misuse of an employer’s resources, namely any violations that lead to financial or reputation damage of the company through the fault of employees.

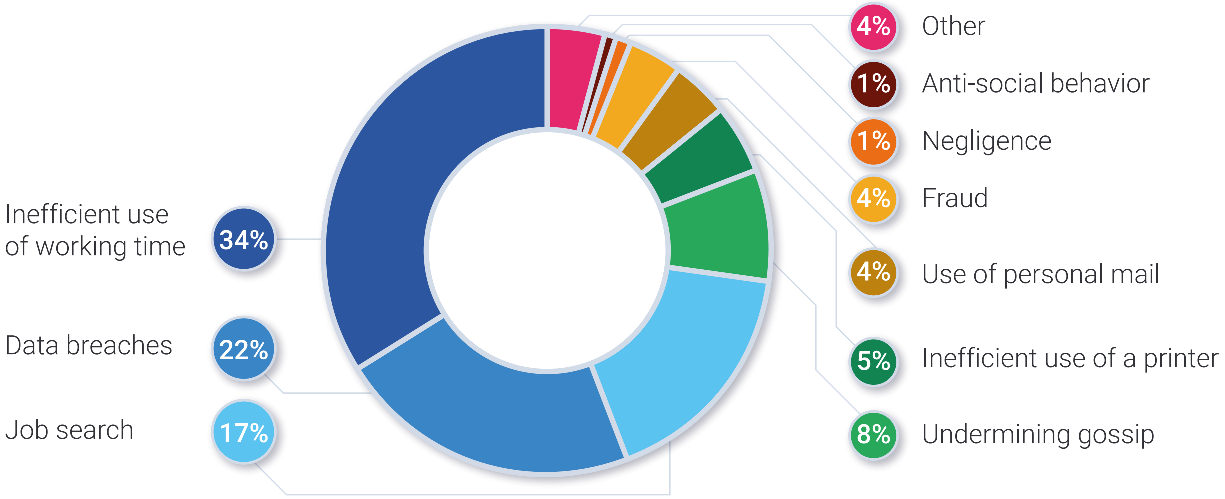
SearchInform has collected anonymous data from its clients using SearchInform services, thus having analyzed the data of 50 small and medium-sized companies. The reports included information about any violation of the company's security policies. Therefore, the analyzed information is not biased and is an objective reflection of the situation in the organizations.

SearchInform analysts have found out how often customers' companies encounter incidents and which of them are most common, the analysis also showcases which channels insiders prefer when attempting to leak sensitive data.

www.searchinform.com

WHAT ARE THE MOST COMMON INCIDENTS?

Every month companies detect at least 25 internal security incidents.



DATA BREACHES

100% of companies registered attempts of leaks.
In most of them, it happens several times a week.

Alexey Parfentiev
Leading analyst at SearchInform:

> – Data leaks can be intentional or accidental (for example, employees can take documents home or upload them to insecure cloud). Violations of discipline towards corporate information, even not deliberate ones, can lead to serious problems for the company. For example, internal orders may become available to all Internet users due to incorrect personal cloud access settings.

22% of all identified incidents are attempts to leak data. In 37% of cases, employees copy large amounts of heterogeneous data they have access to. Most often, employees work with these documents directly.

Alexey Parfentiev:

– Separately, we have analyzed incidents to critical data. When breached a business suffers a number of problems, namely company's know-how, competitive advantage and lucrative contracts are jeopardized, a company might lose valuable employees; moreover, these leaks increase the probability of punishment from the regulator and lead to reputation risks.

WHAT TYPE OF DATA WAS BREACHED MOST OFTEN?

24% **Technical information** – drawings and diagrams; project documentation; layouts; data on product certification; commodity classification; protocols and conclusions of laboratory tests, examinations, etc.

19% **Accounting and financial documents** – financial reporting data; closing documents; accounts; budgets and estimates; information about payroll and bonuses; balance sheets, etc.

6% **Legal documents** – contracts and agreements; charters; registration certificates; forms; orders, etc.

6% **Customer and transaction data** – excerpts or complete customer databases; tender documentation; price lists.

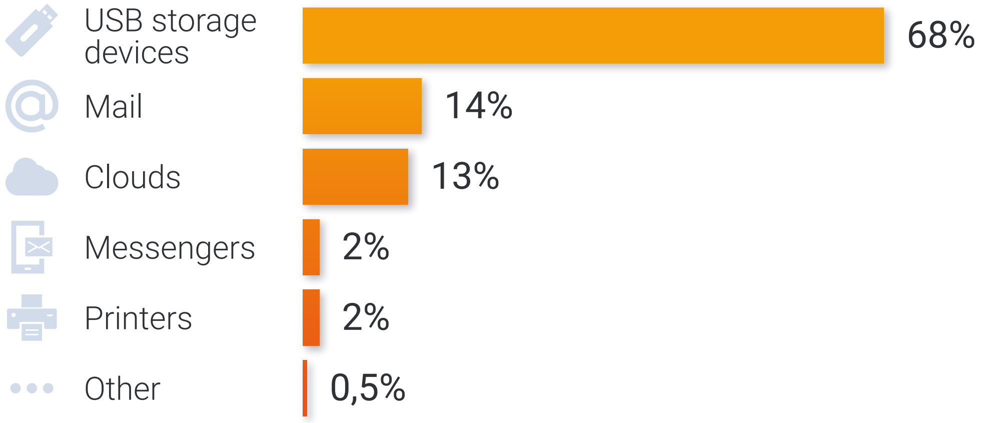
6% **Personal data of clients and employees** – lists of employees; scans of workbooks, insurance certificates and passports; report cards, staffing tables, job descriptions.

2% **Purchases** – technical specifications for conducting purchases; documents with deadlines and delivery points; lists of suppliers.

COMPANIES LOSE CRITICAL DATA ON A REGULAR BASIS

Employees take away technical documentation approximately once a week; accounting, financial, and legal documents are lost every 2 weeks. Customers, employees and transactions data is breached every two months.

THE MOST LIKELY CHANNELS FOR DATA BREACHES



CORPORATE FRAUD

4% of detected incidents represent fraudulent activities. These incorporate theft, shady operations on data, kickbacks accepting, document forgery.

86% of companies deal with attempts to commit fraud.

They are discovered nearly **once a month.**

> **Alexey Parfentiev:**
>
> – Kickbacks accepting in companies are revealed in the process of detecting suspicious negotiations during which an employee speaks or writes about putting one’s “percent”, details which prices should be shown in a commercial offer. Sending documents to third-party contractors, making changes to scans of documents in graphics editing software, etc. are the red flags.

64% of companies

revealed document forgery incidents

The most popular forgery incidents include such violations as changing file creation dates or adding a manager’s signature in a graphics editor. These tricks are observed at least once every two months.

EMPLOYEES WHO POSE THE BIGGEST RISK

Employees who are most likely to be incident causers

36% of companies revealed people prone to anti-social behavior.

More often such behavior patterns get discovered in captured conversations, correspondence about drug or substance abuse, gambling or other addictions.

INEFFICIENT USE OF WORKING TIME

> **Alexey Parfentiev:**
>
> – 100% of inefficient use of working time happens when an employee pretends to work at the computer, meantime spending the lion's share of time in social networks, on entertainment resources or doing their own business. This type of incidents is systematic. If an employee permits oneself to be distracted, he does it all the time.

13% of violators

spend time on non-work related matters every day

2 violators

are estimated to be revealed every week

1-3 hours

is an average time violators spend dealing with off-duty issues at work

8% of cases

of work inefficiency happened due to additional employment or part-time work

MOST COMMON TIME WASTERS

20%	Social networks
17%	News reading
15%	Shopping
11%	Sports betting
10%	Extra job
9%	Games
6%	Search for traveling opportunities
5%	Entertainment resources
2%	Auto and real estate sales
2%	Study, reading books
2%	Youtube and movies
1%	Viewing porn

Social media, web surfing and shopping are main time killers. Employees are estimated to spend from 1 to 3 hours in social networks, reading the news takes 1-2 hours, shopping in its turn takes in about 2 hours of a working day.

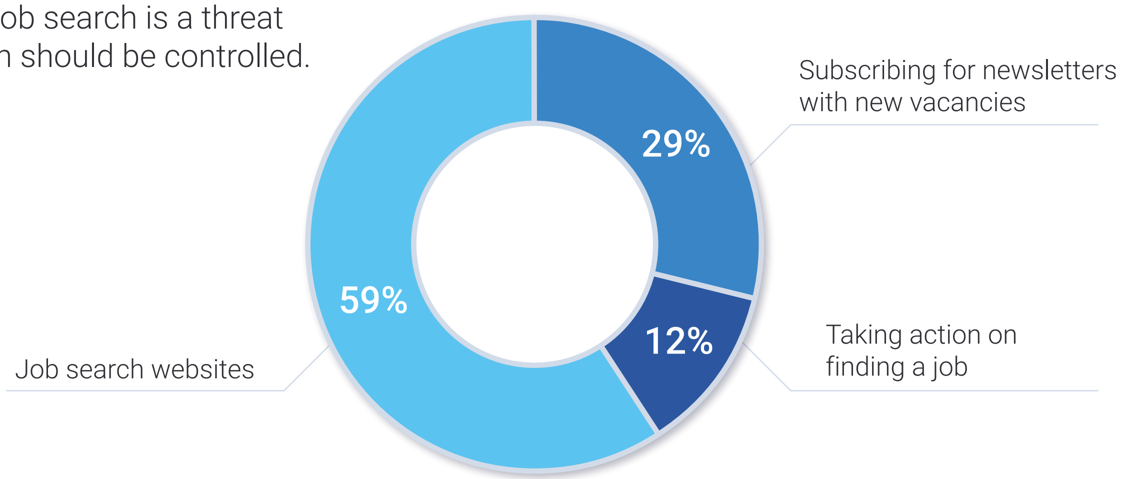
PRINTER MISUSE

> **Alexey Parfentiev:**
>
> – 79% of companies have to face issues with employees who misuse printers at work. 1300 pages of manuals, tutorials, articles are printed on average each month. If you add ink costs, equipment depreciation expenses, money losses will not seem minor to you. The major problem of misusing printers is not even about unaccounted-for costs, it is about the lack of data transfer monitoring as confidential information can be leaked via printers.

JOB SEARCH

100% companies have employees who spend at least some time searching for a job.

This is why specialists mitigating business risks think that job search is a threat which should be controlled.



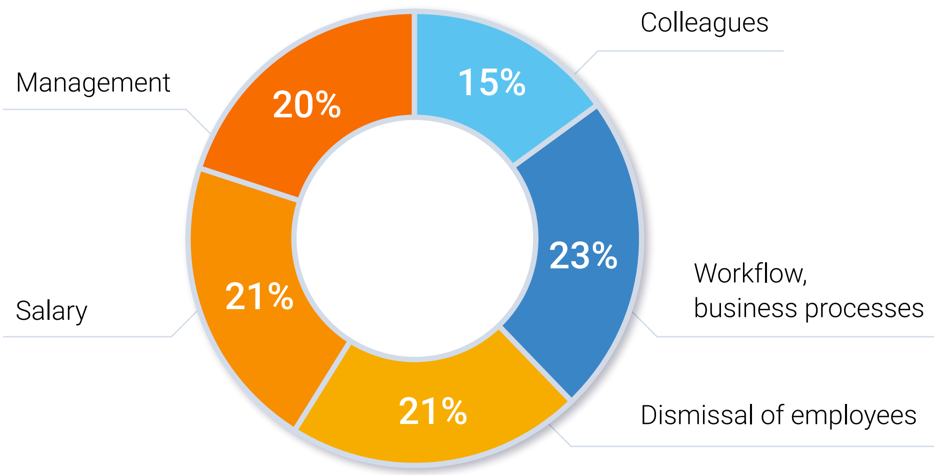
> **Alexey Parfentiev:**
>
> – An employer wants to be aware of employees' willingness to change their job or even determination to find it as soon as possible. A company might lose a valuable professional and promptly deal with personnel shortage. A dismissal of a specialist endangers sensitive information. 40% of companies detect the attempts of remote employees to inflict harm on a company's assets.

ILL-NATURED OPINION

Alexey Parfentiev:

– One out of ten incidents stems from inconsiderate or ill-natured opinions expressed among colleagues, managers. This is a destructive atmosphere which can lead to a decrease in performance, dismissal of employees, blackmail in case specialists responsible for risk mitigation don't pay enough attention.

EMPLOYEES OFTEN MAKE UNDERMINING COMMENTS ABOUT:



METHOD

The research comprises the statistics gathered during the first half of 2020. Incidents in 50 small and medium businesses who use SearchInform services were analyzed. The collected information was anonymized and don't mention the names of the companies which use the services. About 6000 security policy violations were processed and studied. 6 industries are represented by the companies – wholesale and retail, manufacturing, services, IT, construction, fuel and energy.

SearchInform is one of the leading risk management product developers. More than 3000 companies across all major economic domains in 17 countries count on SearchInform regarding an efficient holistic risk management approach. The company offers a number of products to ensure comprehensive threat prevention:

SearchInform DLP

The DLP system protects businesses from data breaches, corporate fraud and other security incidents which happen due to the human factor. In 2017 the system was acknowledged by Gartner and included in the Magic Quadrant.

SearchInform FileAuditor

The DCAP (data-centric audit and protection) solution conducts an automated audit of information storages, discovers access rights violations and monitors changes made to critical data.

SearchInform SIEM

The system for security events collection and analysis in real time, for security incidents detection and ensuring a proactive respond to them.

SearchInform Database Monitor

The DAM (Database activity monitoring) solution provides a company with automated monitoring and audit of operations on databases and business applications.

SearchInform develops the company's services helping organizations with risk management and business risks mitigation tasks implementation. Choosing to use SearchInform services a company solves personnel and expenses issues, as there is no need to hire extra staff to deploy the monitoring solution. Our services allow companies to minimize labor costs and excessive spending on maintaining a company's security at a high level

Visit our blog to be updated on relevant risk management and data safety issues.

linkedin.com/company/searchinform

facebook.com/SearchInformInternational

twitter.com/SearchinformI